IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Applicant:

Paul C. Kocher

Application No.: 09/930,836

Filing Date: August 15, 2001

Title: Cryptographic Computation Using Masking to Prevent Differential Power Analysis and Other Attacks

Confirmation No.: 2389

Group Art Unit: 2132

Examiner: Herring, Virgil A.

Attorney Docket No.: 44424162-8724

INFORMATION DISCLOSURE STATEMENT

SONNENSCHEIN NATH & ROSENTHAL LLP
Customer No. 26263

M/S RCE
Commissioner for Patents
P.O. Box 1450
Arlington, VA 22313-1450

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: M/S RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date below.

March 26, 2007
date of signature

Edward J. Radlo
Edward J. Radlo, Reg. No. 26,793

Sir:

Pursuant to the provisions of 37 CFR § 1.56 and §1.97-§1.98, Applicants hereby submit patents, publications or other information enclosed herewith and listed on the enclosed Form PTO/SB/08A of which they are aware, which they believe may be material to the examination of this application and in respect of which there may be a duty to disclose. This IDS is being filed simultaneously with a Request for Continued Examination under §1.114.

A list of the patents and publications is set forth on the attached Form PTO/SB/08A. A copy of each of the items on the PTO/SB/08A is supplied herewith, except for the four issued United States Patents.

All of the documents were cited in at least one opposition filed against a related European patent, and were first communicated from our foreign associate to the undersigned in February 2007.

While the information and references disclosed in this Information Disclosure Statement may be "material" pursuant to 37 CFR § 1.56, submission of this IDS is not intended to constitute an admission that any patent, publication or other information referred to herein is "prior art" for this invention unless specifically designated as such.

In accordance with 37 CFR § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 CFR § 1.56(a) exists. It is submitted that this Information Disclosure Statement complies with 37 CFR § 1.98 and MPEP § 609, and the Examiner is respectfully requested to consider the listed references.

The Commissioner is hereby authorized to charge our Deposit Account No. 19-3140 for any fees required in connection with the filing of this Information Disclosure Statement. This sheet is being submitted in duplicate.

Respectfully submitted,

date of signature: March 26, 2007

Edward J. Radlo
Reg. No. 26,793
Attorney of Record

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, Illinois 60606-1080
(415) 882-2402

cc: IP/T docket CH (w.PTO/SB/08A)
J. Yang (DPA-DES-CON1) (w.PTO/SB/08A)

14539047

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 4

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Herring, Virgil A
Attorney Docket Number	44424162-8724

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- 5,412,730	05-02-1995	Jones	
		US- 5,483,598	01-09-1996	Kaufman et al.	
		US- 5,764,766	06-09-1998	Spratte	
		US- 5,946,397	08-31-1999	M'Raihi et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		WO 97/13342	04-10-1997	GEM-PLUS S.C.A.		
		WO 98/52319	11-19-1998	Yeda Research and Development Co.		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 4

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Herring, Virgil A
Attorney Docket Number	44424162-8724

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		"Announce: Timing Cryptanalysis of RSA, DH, DSS", sci.crypt newsgroup postings, 13-15 December 1995.	
		"Digital Signature Standard (DSS)", Federal Information Processing Standards Publication 186, 19 May 1994, downloaded: 22 January 2007, website: http://www.itl.nist.gov/fipspubs/fip186.htm	
		"EUROCRYPT '97 Rump Session Program", May 13, 1997, Konstanz, Germany, downloaded: 29 January 2007, website: http://www.iacr.org/conferences/ec97/rump.html	
		"Kocher Algorithm", sci.crypt newsgroup postings, Google Groupes, 12 March 1996, http://groups.google.fr/group/sci.crypt/browse_thread/thread/240f02445602362e/644d5300cdbbf7e3?lnk=gst&q=%q=%22Kocher+Algorithm%22&rnum=1&ht=fr#644d5300cdbbf7e3	
		"Public-Key-Algorithm for Digital Signature", National Institute of Standards and Technology, August 1991, pp. 553-564 (German translation).	
		ANDERSON et al., "Robustness Principles for Public Key Protocals", LNCS 963, Proc. Crypto '95, 1995, pp. 236-247.	
		ANDERSON, Ross, "Two Remarks on Public Key Cryptology", Computer Laboratory, University of Cambridge, Technical Report, Number 549, December 2002, ISSN 1476-2986.	
		BEKER et al., "Key Management for Secure Electronic Funds Transfer in a Retail Environment", Proc. Crypto '84, Springer-Verlag, 1998, pp. 401-410.	
		BONEH et al., "On the Importance of Eliminating Errors in Cryptographic Computations", Journal of Cryptology, 2001, Vol. 14, No. 2, pp. 101-119.	
		BOVELANDER, Ernst, "Smart Card Security 'How Can We Be So Sure?'", COSIC '97 Course, Incs 1528, Springer-Verlag, 1998, pp. 333-337.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 4

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Herring, Virgil A
Attorney Docket Number	44424162-8724

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		BURMESTER et al., "A Secure and Efficient Conference Key Distribution System", LNCS 1189, Proc. International Workshop on Security Protocols, 1996, Springer-Verlag, 1998, pp. 275-286.	
		DAEMEN, Joan, "Management of Secret Keys: Dynamic Key Handling", LNCS 1528, Proc. COSIC '97 Course, Springer-Verlag, 1998, pp. 264-276.	
		FRANKEL et al., "Proactive RSA", Sandia Report SAND96-0856, April 15, 1996.	
		GENNARO et al., "Robust Threshold DSS Signatures", LNCS 1070, Proc. Eurocrypt '96, Springer-Verlag, 1998, pp. 354-371.	
		GILLOGLY et al., "Notes on Crypto '95 Invited Talks by R. Morris and A. Shamir", Cipher 9, 18 September 1995, http://www.leee-security.org/cipher/confreports/conf-rep-Crypto95.html	
		HERZBERG et al., "Proactive Secret Sharing Or: How to Cope with Perpetual Leakage", LNCS 963, Proc. Crypto '95, Springer-Verlag, 1998, pp. 339-352.	
		JABLON, David P., "Strong Password-Only Authenticated Key Exchange", Computer Communication Review, September 25, 1996, Vol. 26, No. 5, pp. 5-26.	
		KOCHER, P., Message: "Re: Timing cryptanalysis of RSA, DH, DSS (Tomazic, RISKS 17.59", The Risks Digest, Forum on Risks to the Public in Computers and Related Systems, Volume 17: Issue 60, 3 January 1996, downloaded: 23 January 2007, website: http://catless.ncl.ac.uk/Risks/17.60.html	
		MATSUMOTO et al., "Speeding Up Secret Computations with Insecure Auxiliary Devices", LNCS 403, Proc. Crypto '88, Springer-Verlag, 1998, pp. 499-506.	
		NACCACHE et al., "Can D.S.A. be Improved?" -Complexity Trade-Offs with the Digital Signature Standard-", LNCS 950, Proc. Eurocrypt '94, 1995, Springer-Verlag, 1998, pp. 77-85.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 4

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Herring, Virgil A
Attorney Docket Number	44424162-8724

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		NACCACHE, David, "Can O.S.S. be Repaired?" - Proposal for a New Practial Signature Scheme-", LNCS 765, Proc. Eurocrypt '93, 1994, Springer-Verlag, 1998, pp. 233-239.	
		NACCACHE, David, "To Whom it May Concern", Forensic Expert Witness by the Court of Appeal, Paris, 6 December 2006.	
		QUISQUATER et al., "Fast Decipherment Algorithm for RSA Public-Key Crypptosystem", 27th August 1982, Electronics Letters 14th October 1982, Vol. 18, No. 21, pp. 905-907.	
		RANKL et al., "Smart Card Handbook", John Wiley & Sons Ltd., 1997, pp. 66-83, 182-189, 208-217, and 237-272.	
		ROBSHAW et al., "Overview of Elliptic Curve Cryptosystems", RSA Laboratories Technical Note, revised June 27, 1997, downloaded: 23 January 2007, website: http://www.rsasecurity.com/rsalabs/node.asp?id=2013	
		SCHNEIER, Bruce, "Applied Cryptography", 2nd Edition, John Wiley & Sons, Inc., 1996, pp. 525-573 (German translation).	
		SCHNORR, C.P., "Efficient Signature Generation by Smart Cards", Journal of Cryptology, 1991, pp. 161-174.	
		SHAMIR, Adi, "On the Poser of Commutativity in Cryptography", LNCS 85, Proc. 7th Colloquia on Automata, Languages and Programming, 1980, pp. 582-595.	
		STEINER et al., "Diffie-Hellman Key Distribution Extended to Group Communication", Third ACM Conf. Computer and Comm. Security, March 1996, pp. 31-37.	
		YEN et al., "RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault Cryptanalysis", IEEE Transactions on Computers, April 2003, Vol. 52, No. 4., pp. 461-472.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.